УДК 343.98

ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ПОЛУЧЕНИЯ ОБЪЯСНЕНИЙ ОТ ЗАЯВИТЕЛЯ ПО МАТЕРИАЛАМ ПРОВЕРКИ О ХИЩЕНИЯХ В СФЕРЕ ОБОРОТА КРИПТОВАЛЮТ

Д. И. Шнейдерова
Могилевский институт МВД Республики Беларусь,
преподаватель кафедры уголовного процесса и криминалистики
e-mail: galuzodi@mail.ru

Аннотация. *В статье рассматриваются особенности получения объяснений от заявителя по материалам проверки о различных видах хищений в сфере оборота криптовалют, содержание и полнота которых оказывают влияние на выбор дальнейших проверочных действий. Автором обращается внимание на содержание полученных объяснений в зависимости от специфики вида хищения, а также статуса криптовалют в механизме его совершения.*

Ключевые слова: *криптовалюта, хищение, вымогательство, мошенничество, модификация информации, материал проверки, объяснение.*

Annotation. *The article discusses the features of obtaining explanations from the applicant based on the materials of the audit about various types of theft in the sphere of cryptocurrency turnover, the content and completeness of which influence the choice of further verification actions. The author draws attention to the content of the explanations received, depending on the specifics of the type of theft, as well as the status of cryptocurrencies in the mechanism of its commission.*

Keywords: *cryptocurrency, theft, extortion, fraud, information modification, verification material, explanation.*

Эпоха активного развития информационных технологий ознаменовалась для правоохранительных органов Республики Беларусь становлением новых видов киберпреступлений, среди которых можно выделить значительно увеличившийся сектор корыстных преступлений, совершаемых с использованием компьютерного программного обеспечения и сети Интернет. Там, малоисследованным с точки зрения частных криминалистических методик расследования хищений и киберпреступлений видится такой продукт цифровой индустрии, как криптовалюты, которые за счет приобретенного на территории Беларуси имущественного статуса могут выступать как в роли средства совершения и сокрытия преступления, так и в роли предмета преступного посягательства. Анализ возбужденных уголовных дел о хищениях в сфере оборота криптовалют показал, что криптовалюты выступают предметом преступления в таких составах, как вымогательство, мошенничество и хищение путем модификации компьютерной информации, средством — в некоторых видах мошенничества,

где предметом преступного посягательства будут являться безналичные денежные средства или электронные деньги.

Следует отметить, что для хищений в сфере оборота криптовалют характерен заявительный принцип возбуждения уголовных дел, то есть поводом выступает письменное или устное заявление лица, которому хищением причинен имущественный вред. В связи с этим первичные сведения, получаемые от заявителя в ходе дачи им объяснений после регистрации заявления, имеют ключевое значение для определения направлений проведения дальнейшей проверки поступившей информации в целях отыскания оснований, которые могут быть положены в решение о возбуждение уголовного дела.

Получение объяснений заявителя как тактический процесс включает в себя три последовательных этапа: подготовительный, рабочий и заключительный. В рамках подготовительного этапа сотруднику правоохранительных органов, проводящему опрос, надлежит выяснить личные данные заявителя, а также его отношение как участника процесса к совершенному хищению, то есть совершено хищение в отношении самого заявителя (при возбуждении уголовного дела признается потерпевшим) или в отношении иного лица (в последующем — свидетель, что для хищений в сфере оборота криптовалют на сегодняшний день не характерно).

Рабочий этап выступает центральным звеном получения объяснений, в рамках которого заявитель излагает обстоятельства совершенного преступления с указанием источников их подтверждения. Как правило, при свободном рассказе опрашиваемое лицо представляет краткие пояснения, требующие конкретизации с целью установления всей совокупности обстоятельств, необходимых для принятия дальнейших решений в рамках работы по материалу проверки. Так, информация, полученная при даче заявителем объяснений, предопределит комплекс действий, которые могут быть проведены в порядке ч. 2 ст. 173 Уголовно-процессуального кодекса Республики Беларусь для установления достаточных признаков, указывающих на один из видов хищений в сфере оборота криптовалют (например, осмотр места происшествия, осмотр предметов, компьютерной информации, в том числе по месту их нахождения, изъятие устройства в рамках осмотра места происшествия с последующим назначением компьютерно-технической экспертизы) [1].

При этом исходная информация повлияет на выбор не только конкретного следственного действия, но и места его проведения, а также на круг необходимых участников. Так, если компьютер стационарный, то провести его исследование можно по месту нахождения (в жилище заявителя) в рамках осмотра места происшествия. Если устройство переносное, то осмотр может быть осуществлен в кабинете сотрудника правоохранительных органов при условии до-

ступа к сети Интернет в случаях, когда это необходимо. Если доступ к крипт окошельку производится через Интернет (онлайн-кошельки) вне зависимости от того, какое устройство используется, то осмотр можно провести и с устройства сотрудника, подключенного к Сети.

Поскольку хищения в сфере оборота криптовалют представляются высокотехнологичными преступлениями, требующими участия в следственных действиях лиц, обладающих специальными знаниями в сфере IT, то при исследовании устройства в рамках осмотра независимо от места его проведения необходимым с практической точки зрения видится привлечение соответствующего специалиста, который способен оказать помощь в отыскании и правильной фиксации цифровой информации. Кроме того, в рамках осмотра должно быть обеспечено и участие заявителя в целях получения от последнего данных о путях доступа к криптокошельку, входных данных в аккаунт кошелька, демонстрации транзакции, проведенной незаконно, и иных сведений. Следует обратить внимание, что если устройство исследуется в рамках осмотра места происшествия по месту жительства заявителя, то к участию в обязательном порядке привлекаются и понятые.

Так как хищения являются предметными преступлениями, то в рамках рабочего этапа сотруднику надлежит выяснить сведения о собственнике похищенных криптовалют или денежных средств, затраченных на их получение, которым, как правило, выступает сам заявитель. При этом, если хищению были подвергнуты безналичные денежные средства, то установить их принадлежность заявителю до совершенного преступления возможно путем анализа данных банковской организации о приходно-расходных операциях по счетам, зарегистрированным на имя заявителя. Но в случае с криптовалютами ситуация обстоит иначе, поскольку прямые официальные источники, подтверждающие обладание ими на праве собственности заявителем, на практике отсутствуют, что связано со спецификой их эмитирования и обращения. В связи с эти при получении объяснений может возникнуть вопрос, действительно ли заявитель обладал ранее похищенной криптовалютой на праве собственности и его ли имущественным правам причинен вред, поскольку может иметь место введение правоохранительных органов в заблуждение с целью получения материальной выгоды. Исходя из изложенного и сложившейся практики обращения криптовалют, принадлежность последних определенному лицу до момента их хищения может быть установлена только путем исследования криптовалютного кошелька, в котором отражаются все проведенные транзакции со средствами на балансе. При этом до такого исследования в рамках осмотра или экспертизы сотруднику правоохранительных органов необходимо при получении объяснений убедиться, что заявитель владеет информацией о получении доступа к этому

криптокошельку (о его виде и особенностях функционирования, с какого устройства обычно осуществлялся вход, каковы входные данные (логин, пароль, seed-фраза), требуется ли для входа подключение к сети Интернет), о нахождении на его счету криптосредств, способах осуществления транзакций, в рамках какой транзакции произведено незаконное списание, и в каком размере, иными сведениями, касающимися как вопроса собственности, так и совершенного преступления. Следует отметить, что приведенные данные имеют общий характер для всех видов хищений в сфере оборота криптовалют. При этом необходимость выяснения иных сведений зависит от специфики каждого из видов хищений:

1) при вымогательстве: содержание поступившего требования о переводе криптовалют и угрозы в случае его невыполнения; дата, время и способ доведения требования до сведения заявителя; размер выкупа и условия его передачи, включая срок и вид криптовалют; действия пользователя на устройстве, в том числе в сети Интернет, предшествовавшие появлению требования (например, скачивание подозрительных и иных файлов, посещение ранее неизвестных сетевых ресурсов, отмеченный пользователем несанкционированный доступ к аккаунту в социальной сети, поступление незначительного количества криптовалют от неизвестного источника, характерное для «пылевой атаки», и т. д.); если вымогательство сопровождается блокированием доступа к файлам на устройстве или их содержимого, то необходимо установить, какие именно типы файлов подверглись воздействию вируса; было ли выполнено требование заявителем (если да, то в какой криптовалюте и в каком размере) и/или реализована ли угроза преступником, если да, то когда и каким способом;

2) при мошенничестве в случае, если криптовалюты являются предметом хищения: при каких обстоятельствах произошел перевод криптовалют на кошелек мошенника; когда, на какой адрес, с использованием каких программных средств осуществлена транзакция, чем она может быть подтверждена; в чем выражался обман со стороны преступника, либо имеет ли место злоупотребление доверием (в этом случае стороны должны быть знакомы и обладать доверительными отношениями); каким образом заявитель вступил в контакт с преступником, предполагая его добросовестность, с помощью каких источников и средств (например, увидел объявление о продаже товара в криптовалюте на торговой интернет-площадке, вступил в переписку с продавцом-мошенником, после диалога перевел ему криптовалюты, товар не получил, мошенник удалил объявление и скрылся; либо проинвестировал мошеннический SCAM-проект или выступил в качестве залогодателя в преступном кредитном криптосервисе и т. д.); в какой момент заявитель осознал, что был обманут и вторая сторона не будет выполнять свои обязательства; выходил ли мошенник

на контакт с заявителем после совершения хищения, если да, то каким способом, что пояснял;

3) если предметом мошенничества выступали безналичные денежные средства или электронные деньги, а криптовалюты являлись средством реализации преступного умысла, то выяснению подлежат следующие обстоятельства: в каких целях заявитель перечислил денежные средства мошеннику (т. е. в чем заключалась суть обмана, например, покупка на бирже криптовалюты либо инвестирование в ICO-проект и т. д.), каковы были встречные обязательства второй стороны после получения средств; когда и каким способом заявитель вступил в контакт с мошенником, или каким образом он узнал о его предложении совершить сделку или инвестирование (реклама, пост в социальной сети или на форуме, рассылка через почту, по совету знакомых или иных лиц и др.); был ли знаком заявитель с преступником ранее, имел ли с ним доверительные отношения; с какого и на какой счет (электронный кошелек) переводились безналичные денежные средства (электронные деньги), в какой валюте и сумме, когда, сколько переводов осуществлено; какие источники могут подтвердить ответы на приведенные выше обстоятельства; в какой момент и по каким признакам заявитель осознал, что был обманут и мошенник не будет выполнять свои обязательства; был ли контакт с мошенником после совершения хищения, если да, то когда, каким способом, каково его содержание; известно ли ему об иных обманутых этим же мошенником и таким же способом лицах;

4) при хищении путем модификации компьютерной информации: кроме общих вопросов, приведенных для всех видов хищений криптовалют, целесообразно выяснить у заявителя способы и источники хранения учетных данных для доступа к криптокошельку (имело ли место автозаполнение логина и пароля за счет функции «менеджер паролей»); имелся ли доступ у третьих лиц к кошельку, с которого произошло неправомерное списание криптовалют, либо к устройству, на котором возможно осуществить вход, в том числе без ручного ввода учетных данных; в какой момент заявитель обратил внимание на недостачу средств на счету криптокошелька, в каком количестве; была ли им самостоятельно выявлена неправомерная транзакция, может ли предоставить ее хеш и адреса выхода; посещал ли до совершения хищения веб-ресурсы, вызывающие подозрение (некорректно функционировавшие, изменившие привычный дизайн или доменный адрес), где оставлял свои учетные данные от криптокошелька; не ухудшалась ли за последнее время работа устройства, что может быть вызвано фоновым действием программы-шпиона; не предоставлял ли заявитель учетные данные третьим лицам для совершения транзакции в его пользу; не было ли необоснованного срабатывания двухфазной аутентификации, оставленной без внимания заявителем.

На заключительном этапе получения объяснений сотруднику надлежит произвести соответствующее документальное оформление полученных сведений путем составления протокола, а также приобщения к нему документов и предметов (например, распечатанные скриншоты из криптокошелька или переписки в социальных сетях), предъявленных заявителем, в случае наличия таковых.

Таким образом, качество и полнота полученных объяснений являются залогом правильного выбора дальнейших проверочных действий, производство которых поможет выявить основания для возбуждения уголовного дела или принятия иного решения по поступившему заявлению.

---

1. Уголовно-процессуальный кодекс Республики Беларусь [Электронный ресурс] : 16 июля 1999 г. № 295-З : принят Палатой представителей 24 июня 1999 г. : одобр. Советом Респ. 30 июня 1999 г. : в ред. Закона Респ. Беларусь от 26.05.2021 г. Доступ из информ.-поисковой системы «ЭТАЛОН». Вернуться к статье